

UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF WISCONSIN

*In the Matter of the Search of*

A rose gold colored Apple iPhone 7 Plus (model A1661) with cracked touch screen, bearing alphanumeric identifiers FCC ID BCG- e3087A, IC 579c-e3087a on the reverse of the device (hereinafter the "DEVICE"), recovered during the execution of a search warrant at 714 W. Montana Street, Milwaukee, Wisconsin 53215 and currently secured at the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233.

Case Number: 18-m-160 (DEJ)

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

I, Jeffrey Metke, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

A rose gold colored Apple iPhone 7 Plus (model A1661) with cracked touch screen, bearing alphanumeric identifiers FCC ID BCG- e3087A, IC 579c-e3087a on the reverse of the device (hereinafter the "DEVICE"), recovered during the execution of a search warrant at 714 W. Montana Street, Milwaukee, Wisconsin 53215 and currently secured at the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233.

located in the Eastern District of Wisconsin there is now concealed: **Please see attached affidavit, which is hereby incorporated by reference.**

The basis for the search warrant under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of a crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Title 21, United States Code, Sections 841(a)(1) and 843(b).

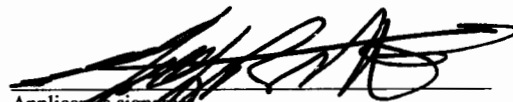
The application is based on these facts:


- ☒ Continued on the attached sheet, which is incorporated by reference.
- ☐ Delayed notice of 180 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me, and signed in my presence.

Date Aug. 30, 2018

City and state: Milwaukee, Wisconsin

  
Applicant's signature  
Name and Title: Jeffrey Metke, U.S. Postal Inspector

  
THE HONORABLE DAVID E. JONES  
United States Magistrate Judge  
Name & Title of Judicial Officer

## **AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Jeffrey R. Metke, being first duly sworn, hereby depose and state as follows:

### **AGENT BACKGROUND AND INFORMATION**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a United States Postal Inspector, assigned to the United States Postal Inspection Service Domicile in Milwaukee, Wisconsin. I have been a federal law enforcement agent for over eleven years. From July 2007 to February 2015, I served as a Special Agent with the United States Department of Homeland Security and from February 2015, to the present day, with the United States Postal Inspection Service. In addition, I have served as a Wisconsin state certified law enforcement officer for multiple agencies in the state of Wisconsin since 1995.

3. The United States Postal Inspection Service is the primary investigative arm of the United States Postal Service and is charged under Title 18, United States Code, Section 3061 with the enforcement of laws governing the use and movement of the United States Mail, including the misuse and fraudulent schemes involving the mail, crimes relating to mail fraud, narcotics trafficking and identity theft involving the United States Mail.

4. I am currently a member of the North Central (formerly Wisconsin) High Intensity Drug Trafficking Area Task Force (HIDTA) assigned to the drug interdiction initiative as an investigator specializing in the smuggling, trafficking, and distribution of dangerous and controlled substances through the United States Mail. I have conducted hundreds of drug investigations in my two decades of law enforcement experience and received continual training in that and other

fields. I am familiar with various methods of smuggling and trafficking narcotics and other controlled substances and the proceeds from sale of such substances. I am also familiar with methods used to evade detection of both the controlled substances and the proceeds from their sale that are used by drug traffickers. Within the United States Postal Inspection Service, a primary investigative assignment of mine is the Prohibited Mail-Narcotics program, which is responsible for protecting the United States Mail from misuse by traffickers and smugglers of illicit controlled substances. Also, this program is engaged in an effort to stop the misuse of the United States Mail by said drug traffickers by seizing the proceeds of this unlawful activity as the proceeds are mailed back to the sources of supply.

5. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

6. Because this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only facts that I believe are sufficient to establish probable cause to believe that the electronic device described herein contains evidence relating to the possession with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1), and/or was used to facilitate the distribution and/or possession with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 843(b).

**I. IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

7. The property to be searched is a rose gold colored Apple iPhone 7 Plus (model A1661) with cracked touch screen, bearing alphanumeric identifiers FCC ID BCG- e3087A, IC 579c-e3087a on the reverse of the device (hereinafter the "DEVICE"), recovered during the execution of a search warrant at 714 W. Montana Street, Milwaukee, Wisconsin 53215 and

currently secured at the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233.

8. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data more particularly described in Attachment B.

## **II. PROBABLE CAUSE**

9. On Wednesday, August 1, 2018, United States Magistrate Judge William E. Duffin authorized a search and seizure warrant for United States Priority Mail Express piece EM085851139US (hereinafter "the parcel"). Your Affiant was the affiant for that search and seizure warrant as well.

10. Upon execution of the search and seizure warrant for the parcel, your Affiant found two brick-shaped bundles covered in concentric layers of cling-style plastic wrap. Each brick contained a white crystalline substance that field tested positive for the presence of cocaine, a Schedule II controlled substance. The two brick-shaped bundles had a combined approximate gross total weight of 2,257 grams. The parcel was addressed in the following manner:

From: Jamie E. Sosa  
345 Calle Sena #114,  
Urb. River Valley  
Canovanas 00729

To: Armando Sosa  
714 W. Montana Street  
Milwaukee, WI 53215

11. On Thursday, August 2, 2018, your Affiant, along with members of the North Central (formerly Wisconsin) High Intensity Drug Trafficking Area Task Force (HIDTA), conducted a controlled delivery of the parcel to the address 714 W. Montana Street, Milwaukee Wisconsin 53215. Your Affiant, acting in an undercover capacity as a U.S. Postal Service letter

carrier, delivered the parcel to the front door of 714 W. Montana Street and scanned the parcel as having been delivered. After the parcel was not picked up by the intended recipients, United States Postal Inspector (USPI) Daniel York retrieved the parcel from the porch of 714 W. Montana Street. Your Affiant had previously completed a United States Postal Service (USPS) Form 3849 (Notice of Re-delivery card), which USPI York left in the mailbox for 714 W. Montana Street. The USPS Form 3849 provided a number for the intended recipient to call to arrange redelivery for the parcel.

12. At approximately 6:30 p.m. on August 2, 2018, a man called the number listed on the USPS Form 3849 card, and left the following recorded message: "Hello, this is Armando Sosa. I call for redelivery to the tracking number EM085851139US for 714 W. Montana Street ZIP code 53215. Please you can redeliver it tomorrow. Thank you." The person who identified himself as "Armando Sosa" had called from telephone number (414) 397-0619 on four occasions that evening. On one occasion, the caller left the above-referenced recorded message requesting redelivery of the parcel.

13. On Monday August 6, 2018, after hearing the message, your Affiant called (414) 397- 0619 and left a message for "Armando Sosa." Within an hour, a person calling from (787) 242-2729, who claimed to be "Armando Sosa" returned your Affiant's call. Your Affiant, who posed as a USPS Customer Service Manager, spoke with the man purporting to be "Armando Sosa," who sought redelivery of the parcel. Your Affiant said that due to a delivery error by the USPS, "Armando Sosa" was entitled to a refund of the postage (i.e., \$93.70). Your Affiant explained that he would need to personally deliver the paperwork necessary for "Armando Sosa" to receive the refund. The man purporting to be "Armando Sosa" agreed, but explained that he had to work until 2:00 p.m. The man purporting to be "Armando Sosa" and your Affiant decided that your Affiant would redeliver the parcel and provide the refund forms to "Armando Sosa" on



August 7, 2018, at 2:30 p.m. Your Affiant thereafter contacted members of the North Central HIDTA to arrange a new controlled delivery of the parcel to 714 W. Montana Street, Milwaukee, Wisconsin 53215 on August 7, 2018, at 2:30 p.m.

14. On August 7, 2018, at approximately 2:30 p.m., your Affiant, dressed as a USPS Customer Service Manager, drove an official marked USPS Delivery Vehicle to 714 W. Montana Street and knocked on the front door of the residence. Members of the North Central HIDTA were simultaneously conducting surveillance. A man subsequently identified as Alvaro PEREZ-MORALES opened the door. Your Affiant inquired, "Mr. Sosa?" PEREZ-MORALES answered, "Yes." Your Affiant said, "I'm Jeff Metke. We spoke yesterday on the phone." PEREZ-MORALES responded, "Ya." With the mailing label facing PEREZ-MORALES, your Affiant handed the parcel to PEREZ-MORALES. Your Affiant said, "Here is your package." PEREZ-MORALES responded "Thanks." Your Affiant handed PEREZ-MORALES a USPS Form 3533 (Application for Refund) and asked, "Mr. Sosa, would you like me to help you fill this out now or would you like to fill this out and bring it to the Post Office?" PEREZ-MORALES responded, "I will bring it to the Post Office." Your Affiant responded, "OK." Your Affiant retrieved the parcel from PEREZ-MORALES in order to scan it as delivered, and then returned the parcel to PEREZ-MORALES, who thanked your Affiant. Your Affiant thanked PEREZ-MORALES and walked to the mail delivery vehicle.

15. After your Affiant delivered the parcel, members of the North Central HIDTA executed an anticipatory search warrant at 714 W. Montana Street, Milwaukee, WI 53215 (hereinafter referred to as "the residence"). During the search, PEREZ-MORALES was located within the residence and detained. PEREZ-MORALES was identified by United States Passport

Number 403832259 as Alvaro PEREZ-MORALES, who was born on July, 24, 1986, in the United States territory of Puerto Rico.

16. During the search of the residence, officers found the parcel and the USPS Form 3533 on the living room floor, and the USPS Form 3849 (Notice of Re-delivery card) on a table in the living room. The officers found PEREZ-MORALES's expired Puerto Rican driver's license, which indicated his residence was in Canovanas, Puerto Rico. Canovanas, Puerto Rico is the city listed on the parcel's return address and where the parcel initially entered the U.S. mail stream. The officers also found a black Motorola mobile telephone with the digits "397-0619" taped to the back of the telephone. The black Motorola mobile phone was found under a sofa in the living room where PEREZ-MORALES was seated. The digits "397-0619" are the last seven digits for the telephone number (414) 397-0619, which was the telephone number "Armando Sosa" purportedly used on August 2, 2018 to request redelivery of the parcel via the undercover Postal Inspection Service telephone line. Furthermore, on the sofa next to PEREZ-MORALES was a Samsung mobile phone and the DEVICE. The officers found an LG mobile phone and a ZTE mobile phone in an upstairs bedroom in the residence as well. North Central HIDTA officers already obtained state search warrants for the Motorola, LG, and ZTE mobile phones, and obtained consent to search the Samsung phone from PEREZ-MORALES's spouse, who claimed ownership of the Samsung mobile phone.

17. The use of fictitious names and fictitious delivery addresses is a common scenario identified by the U.S. Postal Inspection Service in its investigation of the trafficking of illegal drugs and their proceeds through the United States Mail.

18. Your Affiant, and other Postal Inspectors, have identified a trend of drug traffickers mailing controlled substances into the Eastern District of Wisconsin, from states in the western

United States and along the southern international border such as Washington, Oregon, California, Colorado, New Mexico, Texas and Arizona. There, controlled substances are more easily and readily available, due to certain state laws, and a porous international border, among other reasons. Inasmuch as individuals who would receive these controlled substances through the United States Mail are obliged to pay for said controlled substances, often, the United States Mail is utilized by drug recipients to send payments to the West Coast and Southwest drug traffickers. As such, within the Prohibited Mail-Narcotics program area of the United States Postal Inspection Service, certain indicators have been identified in the area of the trafficking of both illegal drugs, and their proceeds, through the United States Mail.

19. Your Affiant, along with other Milwaukee Postal Inspectors, conduct routine examinations of the outside of parcels traveling in Express Mail and Priority Mail Express to the Eastern District of Wisconsin from states on the West Coast and Southwest of the United States looking for indicators of drug trafficking through the United States Mail.

20. Commonplace with drug trafficking through the United States Mail is the use of mobile telephones, particularly Internet-enabled mobile telephones and so-called "smart phones." Based on my training and experience, senders and receivers of parcels containing contraband or evidence of a crime use these devices to communicate and/or transmit, among other things, images of the illicit parcels, tracking numbers, text messages and emails detailing pricing along with the alias names and alias addresses used in the movement of illegal drugs, drug proceeds and other contraband through the U.S. Mail. Furthermore, based on my training and experience, drug traffickers commonly use multiple mobile phones to communicate with their suppliers, their customers, and their families.



21. The DEVICE is currently in the lawful possession of the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233. It came into the north central HIDTA Office's possession following the execution of the anticipatory search warrant at the residence on August 8, 2018 as noted above. Therefore, while the North central HIDTA Office might already have all necessary authority to examine the DEVICE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the DEVICE will comply with the Fourth Amendment and other applicable laws.

22. The DEVICE is currently in storage at the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233. In my training and experience, I know that the DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the DEVICE first came into the possession of the North Central HIDTA Office.

### **III. TECHNICAL TERMS**

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone

numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations.

PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

24. Based on my training, experience, and research, I know that the DEVICE has the capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA and has the ability to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

#### **IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent



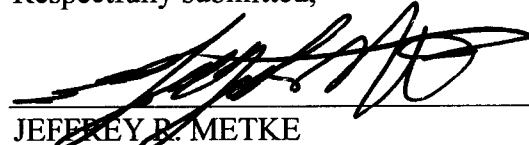
with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



JEFFREY R. METKE  
United States Postal Inspector  
United States Postal Inspection Service

Subscribed and sworn to before me  
on August 30, 2018:



DAVID E. JONES  
UNITED STATES MAGISTRATE JUDGE

### ATTACHMENT A

The property to be searched is a rose gold colored Apple iPhone 7 Plus (model A1661) with cracked touch screen, bearing alphanumeric identifiers FCC ID BCG- e3087A, IC 579c-e3087a on the reverse of the device (hereinafter the DEVICE), recovered during the execution of a search warrant at 714 W. Montana Street, Milwaukee, Wisconsin 53215 and currently secured at the North Central HIDTA Office, located at 801 W. Michigan St., Milwaukee, WI 53233.



## **ATTACHMENT B**

1. All records on the DEVICE described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 843(b), and involve Alvaro PEREZ-MORALES, including, but not limited to:

- a. Electronic drug or money ledgers, drug distribution or customer lists and related identifying information, drug supplier lists (including names, addresses, phone numbers, or any other identifying information); correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- b. Electronic telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, e-mails, documents, and other items or lists reflecting names, addresses, telephone numbers, addresses, and any communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
- c. Records, items and documents stored on the DEVICE reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel from August 2012 to the present;

- d. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, UPS, FedEx, and other mail service receipts and records, bank statements, checks, credit card records, safe deposit box records, records and receipts and rental agreements for storage facilities, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;
- e. Photographs, videotapes or other depictions of assets, co-conspirators, controlled substances, or other activities related to drug trafficking or money laundering; and
- f. Records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.